VOLNÉ GRUPY

<u>Idea</u>: co "největší" grupa generovaná danou množinou X

BYLO: $\langle X \rangle_G = \{ x_1^{k_1} \cdots x_n^{k_n} : x_1, \dots, x_n \in X, k_1, \dots, k_n \in \{\pm 1\} \}$

$\rightsquigarrow$ CHCI: grupa "slov", skládání slov za sebe,
pouze "krácení" vynucené axiomy grup

<u>Konstrukce</u>: <u>def.</u>: slovo nad abecedou A $\equiv$ konečná posloupnost znaků

Př.: $A = \{a, b\}$ $\rightsquigarrow$ slova $a, b, ab, ba, abbaaab, \dots$

povoluje se <u>prázdné slovo</u> ε

X množina $\rightsquigarrow$ $F_X := \left(\text{slova nad } X \cup X^{-1} / \sim, *, {}^{-1}, \varepsilon \right)$

kde $w \sim w'$ $\Leftrightarrow$ ze slova w získám slovo w' vsunutím / vypuštěním dvojice xx^{-1} / $x^{-1}x$

$[w] * [w'] := [ww']$ — spojení posloupností

$[w]^{-1}$: $w = x_1^{k_1} \cdots x_n^{k_n} \Rightarrow [w]^{-1} = [x_n^{-k_n} \cdots x_1^{-k_1}]$

Značení: závorky [ ] se vypouštějí, $aa \rightsquigarrow a^2$, $a^{-1}a^{-1}a^{-1} \rightsquigarrow a^{-3}$ apod.

<u>Př.</u>: $X = \{a, b\}$ $\quad ab^{-1}a * a^{-1}a^{-1}bb = ab^{-1}aa^{-1}a^{-1}bb = ab^{-1}a^{-1}bb$
$= ab^{-1}a^{-1}b^2$

$F_{\{a\}} \simeq \mathbb{Z}$ ... slova nad $\{a, a^{-1}\}$ ... $aa \cdots a = a^k$ / $a^{-1}a^{-1} \cdots a^{-1} = a^{-k}$ / ε

... skládání slov $\equiv$ sčítání exponentů

$\rightsquigarrow$ izomorfismus je $a^k \mapsto k$

F_X není abelovská kdykoliv $|X| \geq 2$

... $ab \neq ba$ kdykoliv $a \neq b$

Tvrzení: G grupa, $f: X \to G$ zobrazení

$\Longrightarrow \exists!\ \varphi: F_X \to G$ homomorfismus t.ž. $\varphi\restriction_X = f$

Př.: $X = \{a,b\}$, $G = \mathbb{Z}$, $f: \{a,b\} \to \mathbb{Z}$

$a \mapsto 3$

$b \mapsto -2$

$\rightsquigarrow\ \varphi: F_{\{a,b\}} \longrightarrow \mathbb{Z}$

$\varepsilon \longmapsto 0$

$a^2 \mapsto 3+3$

$a^k \mapsto 3k$

$b^\ell \mapsto -2\ell$

$a^{k_1} b^{\ell_1} a^{k_2} b^{\ell_2} \mapsto 3(k_1+k_2) + (-2)(\ell_1+\ell_2)$

atd.

Důkaz: má-li být φ hom., pak nutně musí platit:

$$\varphi(x_1^{k_1} \dots x_n^{k_n}) = \varphi(x_1)^{k_1} \dots \varphi(x_n)^{k_n}$$
$$= f(x_1)^{k_1} \dots f(x_n)^{k_n}$$

$\rightsquigarrow$ pokud existuje, pak nejvýše jeden!

Snadné cvičení: ověřte, že takto definované φ je

1) dobře definované (různé zápisy jednoho slova!)
2) homomorfismus

$\square$

Poznámka: Platí i opačná implikace:

$F = \langle X \rangle$ grupa, $\forall G\ \forall f: X \to G\ \exists!\ \varphi: F \to G$ hom. t.ž. $\varphi\restriction_X = f$

$\Longrightarrow F \simeq F_X$

Idea důkazu: dosaďte $G = F_X$, dokažte, že to jediné φ je izo.

PREZENTACE GRUP

Idea: co "největší" grupa – generovaná množinou X
– jejíž generátory splňují relace R

... např. $X = \{a, b\}$ $R = \{ab = ba\}$ ... dva komutující generátory

intuice: $\mathbb{Z} \times \mathbb{Z} = \langle (1,0), (0,1) \rangle$

... kde ji vzít? vezmi volnou F_X, faktorizuj tak, aby byly splněny ty relace

možná defce: slova$/\sim$ kde $w \sim w'$ pomocí axiomů grup / relací v R

lépe: definovat vhodnou normální podgrupu F_X

def: X množina, $R \subseteq F_X$ množina slov

$\rightsquigarrow$ $\langle X \mid R \rangle := F_X / \langle\langle R \rangle\rangle$ kde $\langle\langle R \rangle\rangle$ je nejmenší normální podgp. obsahující R

prezentace grupy

Př.: $\langle a_1, \dots, a_n \mid \emptyset \rangle = F_{\{a_1, \dots, a_n\}}$

Př.: $\langle a \mid a^n \rangle$ ... slova a^k, $k \in \mathbb{Z}$

vynucuji $a^n = 1$, čili také $a^{-n}, a^{2n}, \dots = 1$

... formálně: $\langle\langle a^n \rangle\rangle = \langle a^n \rangle = \{a^{kn} : k \in \mathbb{Z}\}$

... $F_{\{a\}} / \langle a^n \rangle \simeq \mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$

$a^k \longleftarrow k$

Př.: $\langle a, b \mid aba^{-1}b^{-1} \rangle \simeq \mathbb{Z} \times \mathbb{Z}$

$(k, \ell) \longmapsto a^k b^\ell$

☺ díky $ab = ba$ to bude 1) hom. 2) na

$\parallel$ neformální značení

$\langle a, b \mid ab = ba \rangle$ $w = w' \Leftrightarrow ww'^{-1} = 1$

Cv.: $\langle a,b,c \mid a^3, c^5, ab=ba, ac=ca, bc=cb \rangle \simeq ?$

$[\mathbb{Z}_3 \times \mathbb{Z} \times \mathbb{Z}_5]$

? Jak dokázat, že $\langle X \mid R \rangle \simeq G$?

... chci $f: X \to G$ t.ž. to jediné $\varphi: F_X \to G$

1) je na G ... stačí $G = \langle f(X) \rangle$

2) $\operatorname{Ker} \varphi = \langle\langle R \rangle\rangle$

... prakticky: - najdi generátory G splňující dané relace

$\rightsquigarrow$ hom. $F_X \twoheadrightarrow G$ t.ž. $\operatorname{Ker}\varphi \supseteq \langle\langle R \rangle\rangle$

- dokaž, že $|\langle X \mid R \rangle| \leq |G|$ výčtem slov

Př.: $\langle a,b \mid a^2, b^3, (ab)^2 \rangle \simeq S_3$

... $a=(1\,2)$, $b=(1\,2\,3)$ splňují dané relace

... výčet slov: $\varepsilon, a, b, \underset{\displaystyle b^{-1}}{\overset{\shortparallel}{b^2}}, ab, ba$ & 👁 všechna slova délky 3 lze upravit na kratší

$(aba = a^{-1} = a,\ abb = ab^{-1} = ba, \dots)$

Cv.: $D_{2n} \simeq \langle a,b \mid a^2, b^n, (ab)^n \rangle$

Př.: $\langle a,b \mid a^2, b^2, aba = bab \rangle \simeq S_3$

... $a=(1\,2)$, $b=(2\,3)$ splňují dané relace

... výčet slov: $\varepsilon, a, b, ab, ba, aba$ & 👁 víc ne

Cv.: $S_n \simeq \langle a_1, \dots, a_{n-1} : a_1^2, \dots, a_{n-1}^2,\ a_i a_{i+1} a_i = a_{i+1} a_i a_{i+1},\ a_i a_j = a_j a_i \ \forall |i-j|>1 \rangle$

! Vidíme dvě velmi rozdílné prezentace S_3, je snadné vidět $\simeq$?

Jak vlastně rozhodovat, zda $w = w'$?

Špatné zprávy:

[Boone - Novikov] Neexistuje algoritmus, který by pro
1958 1955

dané X, R, w rozhodl, zda
$w = 1$ v $\langle X \mid R \rangle$.

Důsledek: Neexistuje algoritmus, který by pro
dané X, R rozhodl, zda $|\langle X \mid R \rangle| = 1$
(triviální grupa)

Dk: ? $x = 1 \quad \forall x \in X$?

$\leadsto$ tím spíš nelze čekat existenci algoritmu na $\langle X \mid R \rangle \overset{?}{\simeq} G$

Poznámka: každá (konečná) grupa má (konečnou) prezentaci:

$$G \simeq \langle G \mid R \rangle$$

v podstatě multiplikační tabulka

$$\text{kde } R = \{ abc^{-1} : \underbrace{a * b = c}_{\text{v } G} \}$$

Cv.: kvaternionová grupa $Q_8 \simeq \langle a, b : aba = b,\ bab = a \rangle$

Cv.: $G = \langle X \mid R \rangle$, $H = \langle Y \mid S \rangle$ $\Rightarrow$ $G \times H \simeq \langle X \cup Y \mid R \cup S \cup \{ xyx^{-1}y^{-1} : x \in X, y \in Y \} \rangle$